East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 23 April 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is 'Ransomware'.

In a strange quirk of history the first ever Ransomware attack, 30 years ago, was related to a virus that spread across the world.

In 1989 AIDS researcher, Joseph Popp PhD, distributed 20,000 floppy disks to researchers in 90 countries saying the disks contained a computer based questionnaire to gauge the risk of contracting AIDS. The disks were infected with malware that became known as the digital version of the AIDS virus, (source - Palo Alto Networks). The malware was only activated after the computer was turned on 90 times, displaying a ransom note on the screen demanding between $189 and $378 for a "software lease".

The recent pandemic has seen a growth in the number of ransomware attacks. It is not only Windows systems at risk, attacks against Mac and Linux systems have also been seen.

Ransomware is often delivered in the same way as many other types of malicious software. The steps individuals and organisations can take to protect themselves are below.

Defending against Ransomware

Use layers of defence to give more opportunities to detect malware.

Assume that malware will infiltrate and take steps to limit the impact and plan your response.

Make regular backups and make sure to have up-to-date backups of important files; so it's possible to recover data without having to pay a ransom.

- Test your backups to make sure that the files can be restored.
- Make sure the backup device (external hard drive, USB stick or in a cloud service designed for this purpose.) is not permanently connected to your network or device.
- Cloud syncing services (Dropbox, OneDrive, SharePoint, or Google Drive) should **not** the only backup. They may automatically synchronise the infected file.

Prevent malware being delivered to devices and reduce the likelihood of malicious content through the firewall and block websites that are known to be malicious. Public sector organisations are encouraged to subscribe to the NCSC Protective DNS service; this will prevent users from reaching known malicious sites.

Prevent malware from running on devices, keep all devices well-configured and up to date and install security updates as soon as they become available, enable automatic updates, use the latest versions of operating systems and applications to take advantage of the latest security features

Hot topics

An email purporting to be from Iceland (the retailer) has been reported. The email advertises priority delivery slots for the vulnerable and provides a malicious link.

A new scam has people being asked for personal details to be sent to the suspect (purporting to be their employer), as part of their return to work.

Malware is being spread via a new phishing campaign exploiting the COVID19 crisis. Fake virus advice and free COVID-19 testing is offered, installing the malware via attachments in emails.

Also reported were victims receiving calls 'from their bank' offering to pick up money as a service to vulnerable people due to Covid-19. Cards were collected and funds withdrawn.

Victims reported being told to go to thier bank and withdraw funds 'the suspect then told the victim that if the bank asked further questions, they should say it was to do with COVID 19'.

There are increased reports of use of bogus police/bank employees using push payment fraud tactics, whereby pressure is applied, using implied authority and threats, to cause the victim to move funds to a 'safe account'. It is claimed this is necessary to either to secure their own money or to assist in an ongoing situation involving a crime or fraud.

A recent example involved a member of the public who put the phone down on fake police scammer being told 'not co-operating with police enquiries was an arrestable offence' and that there was a police car outside her house, with two plain clothes detectives in it, that would put her in handcuffs and keep her in custody for 48 hours!

There are a few things to affirm here:

- There is no such thing as a 'safe account'.
- Police and banking representatives will NEVER ask you, either as an investigative or security step, to transfer funds anywhere.
- Police and banking representatives will NEVER apply pressure to ensure your compliance. Only criminals do this.
- Police, banking representatives or other officials will be more than happy to wait whilst you verify their identity.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.

Forward suspicious emails to report@phishing.gov.uk.